| Cybersecurity |
| --- |
| Module 11 Challenge Submission File |

## Network Security Homework

Make a copy of this document to work in, and then fill out the solution for each prompt below. Save and submit this completed file as your Challenge deliverable.

### Part 1: Review Questions

#### Security Control Types

The concept of defense in depth can be broken down into three security control types. Identify the security control type of each set of defense tactics.

1. Walls, bollards, fences, guard dogs, cameras, and lighting are what type of security control?

| They are physical security controls |
| --- |

1. Security awareness programs, BYOD policies, and ethical hiring practices are what type of security control?

| They are administrative security controls |
| --- |

1. Encryption, biometric fingerprint readers, firewalls, endpoint security, and intrusion detection systems are what type of security control?

| This is technical security control |
| --- |

#### Intrusion Detection and Attack Indicators

1. What’s the difference between an IDS and an IPS?

| IDS is a passive system that only detects intrusions and relies on a human who needs to decide how to respond to the threat. IPS is an active system that can detect and respond to intrusions or prevent them. |
| --- |

1. What’s the difference between an indicator of attack (IOA) and an indicator of compromise (IOC)?

| The main difference between IOAs and IOCs is that IOAs are typically used to detect attacks in progress, while IOCs are typically used to detect attacks that have already occurred. |
| --- |

#### The Cyber Kill Chain

Name the seven stages of the cyber kill chain, and provide a brief example of each.

1. Stage 1:

| Reconnaissance. At this stage the attacker gathers information about the target, such as IP address, network topology, operation system, employees contact details etc. That may be physical contacts with employees or scanning the internet with Shodan for example. |
| --- |

1. Stage 2:

| Weaponization. At this stage the attacker creates a malicious payload. Virus or trojan. For example one can use Metasploit to create a payload. |
| --- |

1. Stage 3:

| Delivery. At this stage the attacker delivers the pauload to the target. For example the attacker can send an email to the victim that contains malicious attachment. |
| --- |

1. Stage 4:

| Exploitation. After the payload is delivered to the target it exploits a vulnerability in a target’s system to gain access. So it widens the entrance to the target system. |
| --- |

1. Stage 5:

| Installation. The attacker installs malware in the target’s system to maintain access. For example the attacker can install rootkit to control the target. |
| --- |

1. Stage 6:

| Command and control (C2). The attacker communicates with the malware to issue commands. |
| --- |

1. Stage 7:

| Actions and objectives. The attacker takes planned actions on targets system. For example, stealing data. |
| --- |

#### Snort Rule Analysis

Use the provided Snort rules to answer the following questions:

**Snort Rule #1**

| alert tcp $EXTERNAL\_NET any -> $HOME\_NET 5800:5820 (msg:"ET SCAN Potential VNC Scan 5800-5820"; flags:S,12; threshold: type both, track by\_src, count 5, seconds 60; reference:url,doc.emergingthreats.net/2002910; classtype:attempted-recon; sid:2002910; rev:5; metadata:created\_at 2010\_07\_30, updated\_at 2010\_07\_30;) |
| --- |

1. Break down the Sort rule header and explain what this rule does.

| This rule will trigger an alert if a TCP packet from the EXTERNAL network from ANY port will make a connection to the HOME network with destination ports from 5800 to 5820. We shall see the message "ET SCAN Potential VNC Scan 5800-5820". Following data contains flags to be set in TCP communication, threshold - how many attempts to be done before alert triggers, and where to get more info about the rule (url), |
| --- |

1. What stage of the cyber kill chain does the alerted activity violate?

| This rule relates to reconnaissance stage (gathering information) |
| --- |

1. What kind of attack is indicated?

| If triggered it indicates that someone is probing our ports 5800:5820 to identify systems running VNC services. |
| --- |

**Snort Rule #2**

| alert tcp $EXTERNAL\_NET $HTTP\_PORTS -> $HOME\_NET any (msg:"ET POLICY PE EXE or DLL Windows file download HTTP"; flow:established,to\_client; flowbits:isnotset,ET.http.binary; flowbits:isnotset,ET.INFO.WindowsUpdate; file\_data; content:"MZ"; within:2; byte\_jump:4,58,relative,little; content:"PE|00 00|"; distance:-64; within:4; flowbits:set,ET.http.binary; metadata: former\_category POLICY; reference:url,doc.emergingthreats.net/bin/view/Main/2018959; classtype:policy-violation; sid:2018959; rev:4; metadata:created\_at 2014\_08\_19, updated\_at 2017\_02\_01;) |
| --- |

1. Break down the Sort rule header and explain what this rule does.

| The rule applies to TCP traffic from external HTTP port(s) to any port of our network. The rule triggered if transferred binary files. |
| --- |

1. What layer of the defense in depth model does the alerted activity violate?

| Detection layer |
| --- |

1. What kind of attack is indicated?

| This rule detects download of binary files over HTTP |
| --- |

**Snort Rule #3**

Your turn! Write a Snort rule that alerts when traffic is detected inbound on port 4444 to the local network on any port. Be sure to include the msg in the rule option.

| alert ip any any -> $HOME\_NET 4444 (msg:"Inbound traffic detected on port 4444";) |
| --- |

### Part 2: “Drop Zone” Lab

#### Set up.

Log into the Azure firewalld machine using the following credentials:

* Username: sysadmin
* Password: cybersecurity

#### Uninstall UFW.

Before getting started, you should verify that you do not have any instances of UFW running. This will avoid conflicts with your firewalld service. This also ensures that firewalld will be your default firewall.

* Run the command that removes any running instance of UFW.

| $ sudo systemctl stop ufw  sudo ufw disable |
| --- |

#### Enable and start firewalld.

By default, the firewalld service should be running. If not, then run the commands that enable and start firewalld upon boots and reboots.

| $ sudo systemctl enable firewalld  $ sudo systemctl start firewalld |
| --- |

| **Note**: This will ensure that firewalld remains active after each reboot. |
| --- |

#### Confirm that the service is running.

Run the command that checks whether the firewalld service is up and running.

| $ sudo systemctl status firewalld |
| --- |

#### List all firewall rules currently configured.

Next, list all currently configured firewall rules. This will give you a good idea of what’s currently configured and save you time in the long run by ensuring that you don’t duplicate work that’s already done.

* Run the command that lists all currently configured firewall rules:

| $ sudo firewall-cmd —-list-all |
| --- |

* Take note of what zones and settings are configured. You may need to remove unneeded services and settings.

#### List all supported service types that can be enabled.

* Run the command that lists all currently supported services to find out whether the service you need is available.

| $ sudo firewall-cmd —-get-services |
| --- |

* Notice that the home and drop zones are created by default.

#### Zone views.

* Run the command that lists all currently configured zones.

| $ sudo firewall-cmd —-get-zones |
| --- |

* Notice that the public and drop zones are created by default. Therefore, you will need to create zones for web, sales, and mail.

#### Create zones for web, sales, and mail.

* Run the commands that create web, sales, and mail zones.

| $ sudo firewall-cmd —-permanent —-new-zone web  $ sudo firewall-cmd —-permanent —-new-zone sales  $ sudo firewall-cmd —-permanent —-new-zone mail |
| --- |

#### Set the zones to their designated interfaces.

* Run the commands that set your eth interfaces to your zones.

| $ sudo firewall-cmd —-zone web —-change-interface=eth1  $ sudo firewall-cmd —-zone mail —-change-interface=eth3  $ sudo firewall-cmd —-zone sales —-change-interface=eth2  $ sudo firewall-cmd —-zone public —-change-interface=eth0 |
| --- |

#### Add services to the active zones.

* Run the commands that add services to the public zone, the web zone, the sales zone, and the mail zone.
* public:

| $ sudo firewall-cmd --zone public --add-service http --add-service https --add-service pop3 --add-service smtp --permanent |
| --- |

* web:

| $ sudo firewall-cmd --zone web --add-service http --permanent |
| --- |

* sales:

| $ sudo firewall-cmd --zone sales --add-service https --permanent |
| --- |

* mail:

| $ sudo firewall-cmd --zone mail --add-service pop3 --add-service smtp --permanent |
| --- |

* What is the status of http, https, smtp and pop3?

| allowed |
| --- |

#### Add your adversaries to the drop zone.

* Run the command that will add all current and any future blacklisted IPs to the drop zone.

| $ sudo firewall-cmd —-permanent —-new-ipset=blacklist —-type=hash:ip  $ sudo firewall-cmd —-permanent —-zone=drop —-add-source=ipset:blacklist  $ sudo firewall-cmd —-permanent —-ipset=blacklist —-add-entry=10.208.56.23 —-add-entry=135.95.103.76 —-add-entry=76.34.169.118  $ sudo firewall-cmd —-reload |
| --- |

#### Make rules permanent, then reload them.

It's good practice to ensure that your firewalld installation remains nailed up and retains its services across reboots. This helps ensure that the network remains secure after unplanned outages such as power failures.

* Run the command that reloads the firewalld configurations and writes it to memory:

| $ sudo firewall-cmd —-reload |
| --- |

#### View active zones.

Now, provide truncated listings of all currently **active** zones. This is a good time to verify your zone settings.

* Run the command that displays all zone services.

| $ sudo firewall-cmd —-zone=public —-list-services |
| --- |

#### Block an IP address.

* Use a rich-rule that blocks the IP address 138.138.0.3 on your public zone.

| $ sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="138.138.0.3" reject' |
| --- |

#### Block ping/ICMP requests.

Harden your network against ping scans by blocking icmp ehco replies.

* Run the command that blocks pings and icmp requests in your public zone.

| $ sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="0.0.0.0/0" protocol value="icmp" reject' |
| --- |

#### Rule check.

Now that you've set up your brand new firewalld installation, it's time to verify that all of the settings have taken effect.

* Run the command that lists all of the rule settings. Do one command at a time for each zone.

| $ sudo firewall-cmd --zone=public --list-all  $ sudo firewall-cmd --zone=mail --list-all  $ sudo firewall-cmd --zone=sales --list-all  $ sudo firewall-cmd --zone=web --list-all  $ sudo firewall-cmd --zone=drop --list-all |
| --- |

* Are all of the rules in place? If not, then go back and make the necessary modifications before checking again.

Congratulations! You have successfully configured and deployed a fully comprehensive firewalld installation.

### Part 3: IDS, IPS, DiD and Firewalls

Now, you’ll work on another lab. Before you start, complete the following review questions.

#### IDS vs. IPS Systems

1. Name and define two ways an IDS connects to a network.

| In-line IDS. This is IDS configuration, when the IDS is placed directly on the network data path. It acts as a filter, when all traffic must pass through the IDS before reaching its destination. It can monitor traffic in real time and if needed to take immediate action. |
| --- |

| Port-mirroring IDS (Promiscuous IDS) - when IDS is set up on a side of a network and passively listens to traffic mirrored to it by a router. In this case IDS cannot take immediate action to block or modify traffic. |
| --- |

1. Describe how an IPS connects to a network.

| IPS connected to a network In-line in order to be able to take immediate action |
| --- |

1. What type of IDS compares patterns of traffic to predefined signatures and is unable to detect zero-day attacks?

| This type of IDS is named Signature-based. |
| --- |

1. What type of IDS is beneficial for detecting all suspicious traffic that deviates from the well-known baseline and is excellent at detecting when an attacker probes or sweeps a network?

| This is Anomaly-based IDS |
| --- |

#### Defense in Depth

1. For each of the following scenarios, provide the layer of defense in depth that applies:
   1. A criminal hacker tailgates an employee through an exterior door into a secured facility, explaining that they forgot their badge at home.

| This is Physical security layer |
| --- |

* 1. A zero-day goes undetected by antivirus software.

| Intrusion Detection/Prevention layer |
| --- |

* 1. A criminal successfully gains access to HR’s database.

| Access Control, User Authentication, Database Encryption |
| --- |

* 1. A criminal hacker exploits a vulnerability within an operating system.

| Patch Management, Intrusion Detection/Prevention System |
| --- |

* 1. A hacktivist organization successfully performs a DDoS attack, taking down a government website.

| Network Firewalls, Load Balancers, DDoS Mitigation Services |
| --- |

* 1. Data is classified at the wrong classification level.

| Information Classification Policies, User Training and Awareness |
| --- |

* 1. A state-sponsored hacker group successfully firewalked an organization to produce a list of active services on an email server.

| Network Firewalls, Intrusion Detection/Prevention System |
| --- |

1. Name one method of protecting data-at-rest from being readable on hard drive.

| Disk-encryption |
| --- |

1. Name one method of protecting data-in-transit.

| Traffic layer security |
| --- |

1. What technology could provide law enforcement with the ability to track and recover a stolen laptop?

| GPS tracking, WI-FI tracking, Cellular tracking |
| --- |

1. How could you prevent an attacker from booting a stolen laptop using an external hard drive?

| BIOS configuration can help to prevent booting from an external harddrive. You need to set a strong password for BIOS. |
| --- |

#### Firewall Architectures and Methodologies

1. Which type of firewall verifies the three-way TCP handshake? TCP handshake checks are designed to ensure that session packets are from legitimate sources.

| This type of firewall known as Stateful Firewall |
| --- |

1. Which type of firewall considers the connection as a whole? Meaning, instead of considering only individual packets, these firewalls consider whole streams of packets at one time.

| Next-Generation Firewall |
| --- |

1. Which type of firewall intercepts all traffic prior to forwarding it to its final destination? In a sense, these firewalls act on behalf of the recipient by ensuring the traffic is safe prior to forwarding it.

| Proxy Firewall |
| --- |

1. Which type of firewall examines data within a packet as it progresses through a network interface by examining source and destination IP address, port number, and packet type—all without opening the packet to inspect its contents?

| Packet-filtering Firewall |
| --- |

1. Which type of firewall filters solely based on source and destination MAC address?

| MAC Filtering Firewall |
| --- |

### Optional Additional Challenge Lab: “Green Eggs & SPAM”

In this activity, you will target spam, uncover its whereabouts, and attempt to discover the intent of the attacker.

* You will assume the role of a junior security administrator working for the Department of Technology for the State of California.

* As a junior administrator, your primary role is to perform the initial triage of alert data: the initial investigation and analysis followed by an escalation of high-priority alerts to senior incident handlers for further review.

* You will work as part of a Computer and Incident Response Team (CIRT), responsible for compiling **threat intelligence** as part of your incident report.

#### Threat Intelligence Card

| **Note**: Log in to the Security Onion VM, and use the following **indicator of attack** to complete this portion of the assignment. |
| --- |

Locate the indicator of attack in Sguil based off of the following:

* **Source IP/port**: 188.124.9.56:80
* **Destination address/port**: 192.168.3.35:1035
* **Event message**: ET TROJAN JS/Nemucod.M.gen downloading EXE payload

Answer the following questions:

1. What was the indicator of an attack? (*Hint: What do the details reveal?*)

| Data analysis says that certain behavior was detected. Namely - TCP packet from external network from HTTP port 80 to our home network which corresponds to ET TROJAN JS/Nemucod.M.gen. Downloading of malicious EXE payload detected.  The attacker IP belongs to Vital Technoloji with address in Bursa, Turkey. Attacker used Linux OS, MAC 000C29B939C3.  There was downloaded executable file with inside details corresponding to the above mentioned Trojan. Totally sent 31.328 Bytes of data. File name 40.exe  Infected machine MAC - 000C2992E986 |
| --- |

1. What was the adversarial motivation (purpose of the attack)?

| Data stealing |
| --- |

1. Describe observations and indicators that may be related to the perpetrators of the intrusion. Categorize your insights according to the appropriate stage of the cyber kill chain, as structured in the following table:

| **TTP** | **Example** | **Findings** |
| --- | --- | --- |
| **Reconnaissance** | How did the attacker locate the victim? | Wide-spread email sending. |
| **Weaponization** | What was downloaded? | EXE file with Trojan JS/Nemucod.M.gen |
| **Delivery** | How was it downloaded? | The Trojan was hidden in JavaScript in a ZIP file attached to an email |
| **Exploitation** | What does the exploit do? | It retrieves a Trojan Downloader called Fareit, which in turn download set of files containing Gozi Infostealer, which in turn phones data to commanding server.  Here exploited following wulnerabilities: social engineering, ActiveX control and Java Script holes, |
| **Installation** | How is the exploit installed? | When user opens zipped file attached Java Script activates |
| **Command & Control (C2)** | How does the attacker gain control of the remote machine? | The trojan after activation install additional files which provide control on target machine |
| **Actions on Objectives** | What does the software that the attacker sent do to complete its tasks? | It leaks data to the attacker. |

1. What are your recommended mitigation strategies?

| User training, JavaScript disabling if possible, firewall fine tuning, mail filtering against spam and blocking attachments, user privileges control |
| --- |

1. List your third-party references.

| <https://www.varonis.com/blog/cyber-kill-chain>  <https://www.splunk.com/en_us/blog/learn/cyber-kill-chains.html>  <https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanDownloader:JS/Nemucod>  <https://attack.mitre.org/>  <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/trojan.js.nemucod.thbbfai>  <https://www.crowdstrike.com/cybersecurity-101/malware/trojans/> |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.